On Trajectory Design for Intruder Detection in Wireless Mobile Sensor Networks

Edmond Nurellari, *Member, IEEE*, Daniel Bonilla Licea, *Member, IEEE*, Mounir Ghogho, *Fellow Member, IEEE*, Mario Eduardo Rivero-Angeles

***Abstract*—We address the problem of detecting the invasion of an intruder into a region of interest (ROI) which is monitored by a distributed bandwidth-constrained wireless mobile sensor network (WMSN). We design periodic trajectories for the mobile sensor nodes (MSNs) such that high detection probabilities are obtained while maintaining the MSNs' energy consumption low. To reduce the transmission and processing burden on the MSNs, we propose an operation algorithm based on two modes, $surveying\ mode$ and $confirmation\ mode$. In the former, to efficiently detect the intruder while using little mechanical energy, we optimize the surveying path such that the sensed area is maximized. During this mode, each MSN performs local detection and switches to the confirmation mode if and only if the intruder is suspected to be present. In the confirmation mode, each MSN collects further measurements over a predefined duration to reduce the detection uncertainly. A binary local hypothesis testing is performed at each MSN and only positive test statistics are transmitted to the FC where the ultimate decision is taken. Simulations results show the merits of the proposed two-mode operation algorithm in terms of detection performance and energy efficiency.**

***Index Terms*—Distributed detection, intruder detection, mobile sensor nodes (MSNs), wireless mobile sensor networks (WMSNs).**

I. Introduction

CENTRALIZED detection of a binary event (e.g., the presence of an intruder) by monitoring a region of interest (ROI) is one of the most important applications of wireless sensor networks (WSN) [1], [2], [3]. The sensor node (SN) may be $static$ (i.e., with no movement capabilities) or $dynamic$. Deployed over a field, multiple coordinated SNs report their local observations-based test statistics to a fusion center (FC) which combines them to make a global decision. Different strategies exist depending on whether the SN are static or dynamic, and on how the local test statistics are computed and combined at the FC.

First, consider the case of a wireless $static\ sensor\ network$ (WSSN) where multiple coordinated low-cost $static\ sensor\ nodes$ (SSN) are deployed over a large ROI to detect an event and estimate related parameters of interest. Unfortunately, these SSN often suffer from constrained bandwidth, limited available on-board power and security issues [4]. Furthermore, the local SSN decision process (i.e., local detection performance) itself is subject to various security threats [3], [5], [6], [7]. To deal with some of these challenges, WSSN assisted by mobile robots (MR) have been proposed [8], [9]. The SSNs are tasked with the sensing process while the MR may assist with the deployment, relocation and localization of (some of) the SSNs to improve the overall network performance [10] [11] [12], may act as a cluster head or even a FC [13], or provide a source of energy to refill the depleted batteries of the SSN [14].

In wireless mobile sensor networks (WMSN), all sensor nodes can move. As in WSSN, each mobile sensor node (MSN) generates a local test statistic and forwards it to the FC. In the literature, there has been little focus on WMSN due to its design and operation complexities. It has been shown that mobility alleviates several issues related to sensor network coverage and connectivity [15], [16], [17] but many challenges still remain unmet. The WMSN leverages dynamic coverage [18] to potentially achieve the same performance as SSN having much larger numbers of nodes.

The robotics community has shown some interest in the design of multi-robot systems operating as WMSN for surveillance purposes. For instance, in [19], the authors considered a single robot system to detect as many intruders as possible in a certain area. In [20], the authors use reinforcement learning to devise a decentralized WMSN using a multi-robot system to survey dynamic changes within a ROI. In [21] the authors design a motion planning technique to make a team of robots escort a dynamic target by operating as a mobile virtual fencing which adapts its shape; in this case, the robots orbit around the target. Similar problems are considered in [22] and [23]

To the best of our knowledge, the intruder detection literature dedicated to WMSN is scarce when compared to that dedicated to WSSN. Further, most of the existing work on WMSN for surveillance focus on the interior of the ROI rather than on the perimeter, and the few papers dealing with perimeter surveillance are mostly concerned with small perimeters. In addition, the existing work did not address the energy efficiency of the surveillance process jointly with the design of the surveillance trajectories.

In this work, we investigate the performance of a WMSN,

This work was partly supported by the Engineering and Physical Sciences Research Council through the Project Shaking Tunnel Vision under Grant EP/N03435X/1.

D. Bonilla Licea is with the Department of Cybernetics, Faculty of Electrical Engineering, Czech Technical University in Prague, 166 36, Prague 6, Czech Republic, (e-mail:bonildan@fel.cvut.cz).

E. Nurellari is with the School of Engineering, University of Lincoln, LN67 TS, Lincoln, U.K. (e-mail: enurellari@lincoln.ac.uk).

M. Ghogho is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, U.K., and also with the International University of Rabat, Rabat 11 100, Morocco (e-mail: m.ghogho@leeds.ac.uk).

M. E. Rivero-Angeles is with the National Polytechnic Institute, Mexico, (e-mail: mario.rivero.angeles@gmail.com).

which is composed of N identical MSNs, on the task of detecting an intruder within a ROI. The investigation considers both the energy consumption of the MSNs due to motion as well as the probabilities of detection and false alarm. Our objective is to devise a method to optimize the MSNs surveillance trajectories to achieve high detection probabilities with low MSNs' energy consumption. Furthermore, it is highly desirable to minimize the number of MSNs required to cover the ROI while maintaining high detection performance since MSNs are more expensive than SSN. This work takes this issue into account by aiming to design a WMSN so as to monitor large areas with a detection performance comparable to that of WSSNs.

A. Contributions & Organization

The main contributions of our work are:

(i) First, unlike the WMSN surveillance problems found in the literature, we optimize the MSNs' trajectories simultaneously considering their energy consumption and the WMSN detection performance. We develop a new method to optimize energy-efficient MSNs surveillance trajectories for large perimeters and large number of MSNs. The detection task is based on an operation algorithm consisting of two modes: a $surveying-mode$ and a $confirmation-mode$. We analyze and quantify the effects of the MSN controlled trajectories on the system detection performance. We show that the optimum solution to such mobility control is extremely complex in general as it requires the joint optimization of a cost function with respect to many design elements such as the shape, location and orientation of each MSN's path, velocity profile, and local detection threshold. We then propose a sub-optimum but simple hierarchical optimization approach.

(ii) Second, we derive a practical approximation for the probability of avoidance and based on this, we propose two optimization methods for the spatial MSNs' trajectories configuration, taking into account both the power consumption used in motion as well as the detection performance. We then numerically evaluate the proposed system performance and provide insight into the system design parameters.

The rest of the paper is structured as follows. In Section II, we describe the problem formulation (MSN sensing and local decision), the intruder and the MSN models. In section III, we provide an outline for the proposed solution proposed. Then, the individual behaviors of the MSNs are described in section IV. The optimization of the MSNs within the WMSN is treated in section V. In Section VI, we present the fusion rule used by the FC. In Section V, we discuss the optimization of the WMSN. Section VII presents simulation results. Finally, conclusions are drawn in Section VIII.

B. Notations

$\bar{p}$ denotes the complement of the probability p; $\lfloor a \rfloor$ and $\lceil a \rceil$ are the floor and ceiling functions respectively; $\mathcal{A}\{\mathcal{X}\}$ is the area of the region $\mathcal{X}$; $\mathbf{1}_a$ is the indicator function so $\mathbf{1}_a = 1$ if the statement a is true and $\mathbf{1}_a = 0$ otherwise.

II. Problem Formulation & System Model

In this paper we consider a ROI guarded by a WMSN, which is composed of N MSNs and a FC (see Fig. 1), and which is tasked with intrusion detection. For simplicity, we consider a single intruder that produces a signature signal detectable by the MSNs. In this section, we first describe the intruder's behaviour and then in subsection II-B, we describe the individual MSN model.

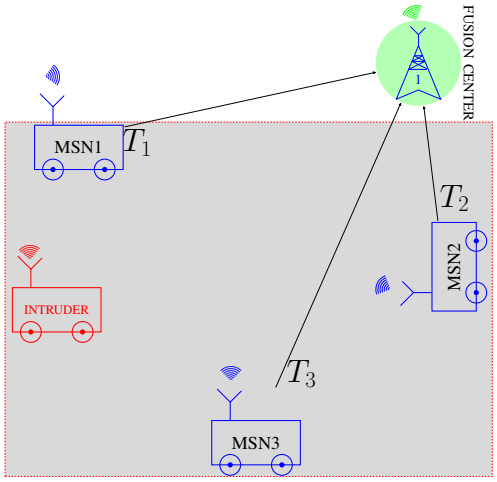

Fig. 1. Schematic architecture of the communication between the MSN and the fusion center (FC). Each MSN generates a test statistic (T_j) by observing the target and can communicate (using $[T_j]$) with the FC only over an energy constrained/bandwidth-constrained link.

A. Intruder

We consider the worst intruder's behavior from the WMSN's perspective: invade the ROI to reach a goal point $\mathbf{p}_g$ (unknown to the WMSN and hence modeled as a random variable uniformly distributed over the ROI) and then escape from the ROI in the shortest possible time.

Assume the intruder to be omnidirectional. Let t_i denote the time when the intruder starts its invasion to the ROI. Its position at time t ($\geq t_i$) is:

$$\mathbf{q}_I(t) = \mathbf{q}_I(t_i) + \int_{t_i}^{t} \mathbf{v}(\tau)\mathrm{d}\tau \qquad (1)$$

where $\mathbf{v}(\tau) \in \mathbb{R}^2$ is the intruder's velocity, with speed ($v_I(\tau) = \|\mathbf{v}(\tau)\|_2$) bounded by $v_I(\tau) \leq v_I$; $\mathbf{q}_I(t_i)$ is the intruder's initial position (located outside the ROI).

We assume that the $intruder$ lacks information about the WMSN. So it is incapable of adapting its trajectory according to the WMSN state. We also assume that the WMSN only knows the maximum speed v_I of the intruder.

We divide the $intruder$'s behavior in two phases:

1) *Invasion phase*: To minimize its time within the ROI, the intruder moves to its goal $\mathbf{p}_g$ at maximum speed v_I along the line passing by $\mathbf{p}_g$ and orthogonal to the ROI's perimeter. The entry point $\mathbf{q}_e$ is the point on the ROI perimeter which is closest to $\mathbf{p}_g$. The intruder's initial point $\mathbf{q}_I(t_i)$is the closest point to $\mathbf{q}_e$ that: i) lies on the

line linking $\mathbf{q}_e$ and $\mathbf{p}_g$; and ii) is outside of the region sensed by the MSNs.

2) *Escaping phase*: The $intruder$ exits the ROI by moving on a straight line at maximum speed to $\mathbf{q}_I(t_i)$ (located outside the sensed region).

For simplicity we neglect the time spent by the intruder at $\mathbf{p}_g$.

B. Mobile Sensor Node

The WMSN is composed of N MSNs. For simplicity, we model the position of the j^{th} MSN ($\mathbf{p}_j(t)$) at time instant t using a single-integrator:

$$\mathbf{p}_j(t) = \mathbf{p}_j(t_i) + \int_{t_i}^{t} \mathbf{u}_j(\tau)\mathrm{d}\tau, \quad \forall_{j=1}^{N} \tag{2}$$

where $\mathbf{u}_j(\tau) \in \mathbb{R}^2$ is the control signal; $\mathbf{p}_j(t_i)$ is the initial position of the j^{th} MSN and $\|\mathbf{u}_j(\tau)\|_2 = v_j(\tau)$ its speed. For simplicity, we also assume that the mechanical energy consumed by the j^{th} MSN from t_i up to t is:

$$E_{mech}(t_i, t, \mathbf{u}_j) = \int_{t_i}^{t} v_j^2(t)\mathrm{d}t. \tag{3}$$

As stated previously, the $intruder$ leaves a signature signal which can be sensed by the MSNs. As in [26], [27], [28], we assume an isotropic signal power attenuation model, and the signature signal is assumed to decay with distance according to a power law. The noise-free signal received by the j^{th} MSN from the $intruder$ can thus be expressed as:

$$\tilde{a}(\mathbf{p}_j[n], \mathbf{q}_I[n]) = \frac{\sqrt{P_I}\mathbf{1}_{(\|\mathbf{q}_I[n]-\mathbf{p}_j[n]\| \leq r)}}{\max(d, \|\mathbf{q}_I[n] - \mathbf{p}_j[n]\|)}, \tag{4}$$

and the output of the j^{th} MSN sensor's is:

$$s_j[n] = \tilde{a}(\mathbf{p}_j[n], \mathbf{q}_I[n]) + w_j[n] \tag{5}$$

where $w_j(n)$ is a zero-mean white Gaussian noise[1] with power σ^2; P_I is the power of the signature signal generated by the intruder; d is the minimum sensing range; r is the maximum sensor's range; $\mathbf{p}_j[n]$ is the discretized version of $\mathbf{p}_j(t)$, i.e. $\mathbf{p}_j[n] = \mathbf{p}_j(n\Delta_s)$ with $n \in \mathbb{N}$ and Δ_s representing the sampling period [26], [27], [28]; similar notations will be used for all the other time-dependent functions in this paper.

The sensor model described in (4) and (5) is a simple model which captures the main aspects of the sensing process: the received signal $a(\mathbf{p}_j[n], \mathbf{q}_I[n])$ is saturated if the distance to the source is smaller than a minimum distance d; the received noise-free signal $a(\mathbf{p}_j[n], \mathbf{q}_I[n])$ is zero if the distance to the source is larger than the sensing range r; the signal measured at the sensor's output is a noisy version of information-bearing signal $a(\mathbf{p}_j[n], \mathbf{q}_I[n])$; the additive noise is assumed to Gaussian and white (which is a good approximation in many practical scenarios).

Though simple, the adopted sensor model is general enough to model the basic high level characteristics of many different types of omnidirectional sensors such as acoustic or electromagnetic sensors, and even more complex sensors such as omnidirectional cameras.

Finally, we denote the surface sensed by the j^{th} MSN at a discrete time instant n as:

$$\mathcal{S}_r(\mathbf{p}_j[n]) = \{\mathbf{q} \mid \|\mathbf{p}_j[n] - \mathbf{q}\| \leq r\}. \tag{6}$$

III. WMSN Optimization Outline

The WMSN is tasked with surveying and detecting intrusions into the ROI. In order to extend its operational lifetime, the MSNs must consume energy efficiently (see (3)) while performing their task. In this paper, we propose a method to optimize the WMSN focusing mainly on the MSNs' trajectories and behaviour.

The goal is design the WMSN to obtain a high probability of detecting the intruder while using the MSNs' energy efficiently. This is an extremely complex problem and so we take a down-top approach. In other words, we start by optimizing the individual behavior of the MSNs in section IV and then optimize the overall configuration of the N MSNs within the ROI in section V. The latter optimization is performed by first determining the number of MSNs to assign to each part of ROI (see section V-A), and then deriving a suitable approximation for the global probability of avoidance (see section V-B).

One key property of our optimization technique is the introduction of the probability of intersection concept (see section V) that will allow us to decouple the optimization of the MSNs' trajectories from that of the parameters directly associated with the detection part of the system, such as the detection thresholds. This property not only simplifies the optimization significantly but also allows to reuse the proposed approach with more elaborated sensor models[2].

IV. MSN behaviour modes

We divide the individual behavior of each MSN in two different operational modes:

- $surveying - mode$: during this operational mode, the MSN tracks a predetermined and periodic trajectory while sensing its environment. We optimize the MSN's trajectory to maximize the covered area under energy consumption constraints. The MSN operates on a low-energy consumption mode with a reduced processing capability to increase its operational time (and thus that of the WSMN). If the MSN's preliminary local sensing suggests an intruder's presence, the MSN switches to its $confirmation - mode$ to confirm or dismiss this hypothesis.
- $confirmation - mode$: this aims to minimize the uncertainty associated with the intruder's status (i.e., present or absent). If the resulting decision is positive, it is transmitted by the MSN to the FC. Then, the MSN switches back to its energy-efficient $surveying - mode$.

The FC continuously listens to the MSNs and collects their transmitted local decisions to produce a global decision on

[1] We assume Gaussian noise for simplicity although in practice the noise may not be Gaussian [31]. Nevertheless we have to mention that this paper focuses on the design of the MSNs trajectory optimization and that minor changes can be done to adapt the proposed method to consider non-Gaussian noise.

[2] If the sensor models are not omnidirectional, the proposed approach can still be used but the individual MSN behaviors should be adapted accordingly.

whether or not an intruder is present in the ROI; details of this are provided in Section VI for details.

The optimization of the surveying and confirmation modes consider both the detection performance and the energy spent due motion. After optimizing the individual behaviors of the MSNs, we will discuss their spatial distribution within the ROI in section V.

TABLE I
WMSN PARAMETERS

N	number of MSNs
N_k^M	number of MSNs for kth ROI side
N_k^P	number of paths for kth ROI side
M_k	number of MSNs sharing the kth path
ℓ_j	length of path associated to jth MSN
$\mathbf{c}_j$	center of path associated to jth MSN
ϕ_j	orientation of path associated to jth MSN
v_j	jth MSN speed during the surveying mode
$\tilde{\Lambda}_j$	$surveying\ mode$ detection threshold for the j^{th} MSN
C	duration of confirmation mode
Λ_j	$confirmation-mode$ detection threshold for the j^{th} MSN
C_f	sliding window size for the FC fusion rule
K	threshold used by the FC

A. Surveying Mode

During the $surveying-mode$, each MSN follows a periodic trajectory[3] in the ROI with period Δ_T. For each MSN, the elements of the surveying mode to optimize are: i) the path's shape; ii) the MSN's location and orientation within the ROI; iii) the MSN's velocity profile; and iv) the threshold used in the local detection. Simultaneously optimizing all of the aforementioned WMSN's elements is in general extremely complex. It is therefore highly desirable to adopt a simpler but suboptimum hierarchical optimization approach.

We start with optimizing the path's shape. The WMSN objective is to detect the intruder efficiently while keeping the consumption of the MSNs' mechanical energy low. So, given a path's length, the sensed area must be maximized. Assuming that the sampling period (Δ_s) is significantly smaller than the trajectory period (i.e., $\Delta_s \ll \Delta_T$), the optimization of the path's shape of the j^{th} MSN can be mathematically stated as follow:

$$\begin{aligned} &\underset{\mathcal{P}_j}{\text{maximize}} \quad \mathcal{A}\{\cup_{t\in[0,\Delta_T]}\mathcal{S}_r(\mathbf{p}_j(t))\} \\ &\text{s.t.} \\ &\mathcal{P}_j = \{\mathbf{p}_j(t)|t\in[0,\Delta_T]\} \\ &\mathcal{L}\{\mathcal{P}_j\} = \ell_j \end{aligned} \tag{7}$$

where $\mathcal{P}_j$ is the candidate path for the jth MSN and $\mathcal{L}\{\mathcal{P}_j\}$ is the length of $\mathcal{P}_j$. Solving (7) is equivalent to minimizing the distance traveled by the MSN (and equivalently its mechanical energy consumption) for a given sensed area.

To solve (7), as adopt an approach similar to that of [16]. For a fixed path's length ℓ_j, the optimum shape is a straight line, see Fig. 2. The boundary of the convex hull of the sensed region is marked in red dashed line. We will refer to such a path as the $surveying\ path$.

[3]The trajectory consists of both a path and an associated velocity profile.

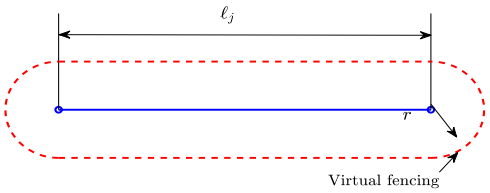

Fig. 2. A schematic of the optimum path (blue line) and the boundary of the sensing region associated to this path (red dashed line).

After optimizing the surveying path's shape, we determine the MSN's velocity profile. Since the MSN's trajectory is set to be periodic with period Δ_T, the MSN must go back and forth along the surveying path. Using calculus of variations [30], we optimize the MSN speed profile to minimize its energy consumption (3) subject to its motion model (2). The result is that during the surveying mode, the MSN must move with constant speed. Hence, in the rest of the paper, we will consider constant speed for all MSNs when operating on the surveying mode; so, to alight the notations we will write v_j instead of $v_j(t)$.

During the surveying mode, the MSN follows its optimum surveying path with constant speed while simultaneously sensing its environment, see appendix A. The optimization of the other parameters of the surveying mode will be considered in section V.

B. Confirmation Mode

The main objective of the confirmation mode is to confirm or refute the intruder's suspected presence arisen during the surveying mode. So, in this mode, the MSN improves its sensor's signal-to-noise ratio (SNR) (5) to reduce the uncertainty about the intruder's presence hypothesis.

To design the confirmation mode, we first calculate the sensor's output power assuming the intruder to be within the sensing region of the MSN, i.e., $\mathcal{S}_r(\mathbf{p}_j[n])$. For convenience, let us define two variables (only used in this subsection and in Appendix B to describe the confirmation mode behaviour): t_i^j as the $intersection\ time$— the time when the $intruder$ enters the jth MSN sensing region (i.e., $\mathcal{S}_r(\mathbf{p}_j(t_i^j))$) just before the MSN switches to the confirmation mode; and $n_d^j\Delta_s$ as the first sampling instant of the jth MSN during the confirmation mode. Note that $n_d^j\Delta_s \geq t_i^j$.

The positions of both the j^{th} MSN and the $intruder$ for $n \geq n_d^j$ are :

$$\begin{aligned} \mathbf{p}_j[n] &= (\Delta_s n - t_i^j)v_j\left[\cos(\psi_j[n-1])\ \sin(\psi_j[n-1])\right]^{\mathrm{T}} \\ &+ \mathbf{p}_j(t_i^j), \\ \mathbf{q}_I[n] &= (\Delta_s n - t_i^j)v_I\left[\cos(\theta[n-1])\ \sin(\theta[n-1])\right]^{\mathrm{T}} \\ &+ r\left[\cos(\omega_j)\ \sin(\omega_j)\right]^{\mathrm{T}} + \mathbf{p}_j(t_i^j) \end{aligned} \tag{8}$$

where $r\left[\cos(\omega_j)\ \sin(\omega_j)\right]^{\mathrm{T}}$ is the intruder's position relative to the jth MSN at time t_i^j; $\left[\cos(\psi_j[n-1])\ \sin(\psi_j[n-1])\right]^{\mathrm{T}}$ and $\left[\cos(\theta[n-1])\ \sin(\theta[n-1])\right]^{\mathrm{T}}$ are the MSN's and intruder's movement directions respectively, see Fig. 3.

For simplicity, we assume the intruder's goal point $\mathbf{p}_g$ to be far from $\mathcal{S}_r(\mathbf{p}_j(t_i^j))$ (this is reasonable since, in general,

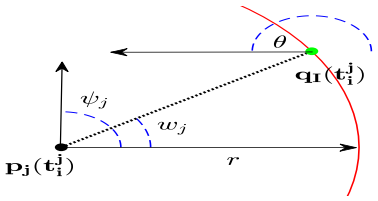

Fig. 3. jth MSN (black dot) and intruder (green dot) positions at time t_i^j. In red the sensing range of the MSN. The angles ϕ_j and θ describe the movement directions for the MSN and the intruder while ω_j is the angular position of the intruder with respect to the MSN at time t_i^j.

the ROI is much larger than $\mathcal{S}_r(\mathbf{p}_j(t_i^j))$). This implies that the intruder's direction remains constant close to time t_i^j. Hence, $\theta[n-1]$ is constant, and so we subsequently use θ to alight notation.

We assume $d \ll r$ in (4) and also $\|\mathbf{p}_j(n) - \mathbf{q}_I(n)\| \leq r$ (this is true after time $n_d^j \Delta_s$ but close to it). Then, from (4) we obtain:

$$\mathbb{E}\left[\tilde{a}^2(\mathbf{p}_j[n], \mathbf{q}_I[n])\right] \approx \mathbb{E}\left[\frac{P_I}{\|\mathbf{q}_I[n] - \mathbf{p}_j[n]\|^2}\right] \tag{9}$$

where the expected value is taken with respect to θ and ω_j. By applying Jensen's inequality to the r.h.s. of (9), we obtain:

$$\mathbb{E}\left[\frac{P_I}{\|\mathbf{q}_I[n] - \mathbf{p}_j[n]\|^2}\right] \geq \frac{P_I}{\mathbb{E}\left[\|\mathbf{q}_I[n] - \mathbf{p}_j[n]\|^2\right]} \tag{10}$$

Using (8) and after some simple algebra we have that:

$$\begin{aligned} \|\mathbf{p}_j[n] &- \mathbf{q}_I[n]\|^2 \\ &= (n\Delta_s - t_i^j)^2 \left(v_j^2 + v_I^2 - 2v_j v_I \cos(\psi_j - \theta)\right) \\ &+ 2(n\Delta_s - t_i^j) r v_I \cos(\omega_j - \theta) \\ &- 2(n\Delta_s - t_i^j) r v_j \cos(\psi_j - \omega^j) + r^2. \end{aligned} \tag{11}$$

As it will be shown in section V, the MSNs will follow a path along the perimeter of the ROI. From the description of the intruder's behaviour in section II-A, it is evident that the intruder's movement will be orthogonal to the ROI's perimeter and thus to the MSN's path. Hence $\cos(\psi_j - \theta) = 0$. Also, we have that $\mathbb{E}[\cos(\omega_j - \theta)] = 0$ and $\mathbb{E}[\cos(\psi_j - \omega_j)] = 0$ because the intersection of the intruder with the MSN's sensing region can occur during any of the two intruder's phases (invasion and escaping phases) with the same probability due to the MSN's periodic trajectory and the symmetry of the problem. Hence, we obtain a lower bound for (9):

$$\frac{P_I}{\mathbb{E}\left[\|\mathbf{q}_I[n] - \mathbf{p}_j[n]\|^2\right]} = \frac{P_I}{\Delta_s^2 (n - n_d^j)^2 (v_j^2 + v_I^2) + r^2} \tag{12}$$

Maximizing the r.h.s. of (12) instead of the original objective function (i.e., $\mathbb{E}\left[\tilde{a}^2(\mathbf{p}_j[n], \mathbf{q}_I[n])\right]$) will yield a sub-optimum but simpler solution to the MSN trajectory design during the confirmation mode. This is clearly achieved by setting to zero the j^{th} MSN's speed; i.e., $v_j = 0$.

We conclude this subsection by noting that the optimum operation of the confirmation mode is for the MSN to stand still for $C\Delta_s$ seconds(C is a design parameter to be discussed later) to confirm or infirm the presence of the intruder. It is worth pointing out that if the MSN had more knowledge about the intruder's behavior and if we take into account the MSN's location within the ROI and the sensors' measurements of the other MSNs, a more efficient confirmation mode might be be obtained.

The local detection executed during the confirmation mode is discussed in Appendix B. If this detection indicates the presence of an intruder, then the MSN transmits its decision to the FC. The transmission from the MSNs to the FC are assumed to be error free (see e.g., [3], [24], [25]).

After discussing the individual surveying and confirmation modes of the MSNs, we will next discuss the organization of the MSNs within the WMSN.

V. MSNs Configuration

To complete the design of the WMSN, we need to discuss the organisation/coordination of the MSNs and the FC fusion rule.

Given the individual MSNs' surveying and confirmation modes (described in section IV), the WMSN's performance— given by the global probability of detection (P_d^g) which we define as the probability that the FC detects the $intruder$ when it invades the ROI— depends on the MSNs' trajectories and the detection-related elements.

The trajectory elements of each MSN are the MSN's speed during the surveying mode, and the center, orientation and length of its surveying path. The detection-related elements are the local thresholds used by the MSN to switch from the surveying to the confirmation mode, the confirmation mode's duration and the threshold to confirm the intruder's presence.

We wish to design the WMSN so as to maximize the global probability of detection (P_d^g). However, in order to simplify the problem and get useful insights, we first decouple the optimization of the MSN trajectory elements from that of the detection-related elements. To do this, we design the MSN trajectories so as to maximize the global probability of intersection (P_{GPI}) which is defined as the probability that the intruder comes within sensing range of at least one MSN for at least one sampling instant:

$$\mathrm{P}_{GPI} \triangleq \Pr\left(\exists\{n, j\} : \|\mathbf{q}_I[n] - \mathbf{p}_j[n]\|_2 \leq r\right) \tag{13}$$

with $j \in \{1, 2, \cdots, N\}$.

If, and only if, the MSNs used noiseless sensors the global probability of detection P_d^g would be equivalent to the global intersection probability P_{GPI}. The presence of noise in the sensors degrades the probability of detection. Hence, P_{GPI} is an upper bound for P_d^g. We also define the global probability of avoidance (P_{GPA}) as the complement of P_{GPI} (i.e., $\mathrm{P}_{GPA} = \bar{\mathrm{P}}_{GPI}$).

We consider the ROI to be a convex polygon of center $\mathbf{c}_{ROI}$ and N_S sides of lengths $\{L_k\}_{k=1}^{N_S}$ with $\min_k(L_k) \gg r$. To further simplify the problem, we constraint the MSNs to fully cover the ROI perimeter. This will ensure that there is no possibility for the intruder to get into the ROI without risking being detected while minimizing the overall total distance traveled by the MSNs. This will reduce the MSN energy consumption and will increase the lifetime of the WMSN.

To achieve this, we constraint the union of all the MSN paths (denoted as $\mathcal{P}_{MSN}$) to have the same shape and orientation as $\mathcal{P}_{ROI}$, to be centered at $\mathbf{c}_{ROI}$, and also designed so that the distance between the corresponding vertices and $\mathcal{P}_{ROI}$ to be equal to the sensing range r, (see Fig. 4).

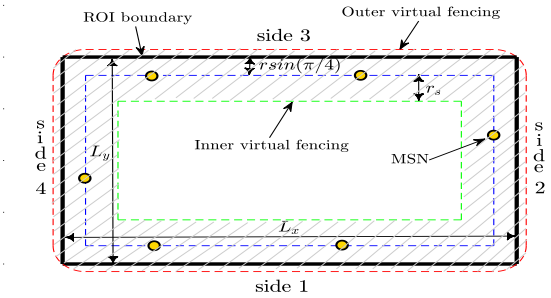

Fig. 4. Schematic of the MSNs' surveying paths: the black rectangle represents the ROI; the blue rectangle represents the MSNs' surveying paths; the red and green rectangles represent the outer virtual fencing and the inner virtual fencing respectively.

In the next section we discuss how to determine the number of MSNs assigned to each side of $\mathcal{P}_{MSN}$. For this, we assume $N \geq N_S$. Then, in subsection V-B we discuss the optimization of the MSNs' trajectories.

A. MSNs' Deployment Rule

We will deploy the N MSNs along $\mathcal{P}_{MSN}$. The first step is to determine the number N_k^M of MSNs allocated to the kth side of $\mathcal{P}_{MSN}$ with length L_k. We propose two guidelines to determine N_k^M: one MSN per ROI side, which ensures that all the ROI sides are guarded; and N_k^M must be proportional to L_k, which ensures that larger ROI sides are surveyed by more robots.

For simplicity, in the rest of the paper, we consider a rectangular ROI of side lengths $L_k = L_x$ for $k = 1, 3$ and $L_k = L_y$ for $k = 2, 4$. From the previous guidelines, we propose [4] $N_k^M = \lfloor \frac{NL_y}{2(L_x+L_y)} \rfloor$ for $k = 2, 4$ and $N_k^M = \lceil \frac{NL_x}{2(L_x+L_y)} \rceil$ for $k = 1, 3$. Note that $L_x > L_y$, see Fig. 4.

Once we have determined $N_k^P \leq N_k^M$, we divide the kth side of $\mathcal{P}_{MSN}$ into N_k^P different non-overlapping paths. Let N^P be the total number of different paths.

Note that $N_k^P \leq N_k^M$ implies that two or more MSNs can share the same path. For simplicity, we limit the number of MSNs sharing one path to two. When two MSNs share the same path, according to extensive simulations (see results in section VII), the intersection probability increases if both MSNs follow synchronized and mirrored trajectories rather than independent ones. This synchronization is obtained by ensuring that: i) the initial positions of both MSNs are symmetric with respect to the path's center; ii) both MSN speeds are identical; iii) the MSNs' directions of movement are opposite to each other; and iv) when one MSN switches from its $surveying\ mode$ to its $confirmation\ mode$, the other MSN also switches its behavior mode to maintain both trajectories synchronized.

After determining N_k^M we need to determine both $\{N_k^P\}_k$ and the number of MSNs per path. According to simulations, the following heuristic is a convenient way to determine those numbers to significantly reduce the probability of avoidance:

(i) if N_k^M is even then $N_k^P = N_k^M/2$ and each path of the kth side surveyed by two MSNs.

(ii) if N_k^M is odd and $N_k > 3$ then $N_k^P = (N_k^M - 1)/2 + 1$. If N_k^P is odd then two MSNs are assigned to each path, except the central path that is surveyed by one MSN. If N_k^P is even, then two MSNs are assigned to each path, except the path $N_k^P/2$ that is surveyed by one MSN.

(iii) if $N_k^M = 3$ then $N_k^P = 2$; two MSNs are assigned to the first path and one MSN to the second one.

The above procedure is heuristic but it reasonably determines the number of MSNs per path, the number of MSNs per side and the number of paths per side.

B. MSN's Trajectory Configuration

In Section V-A, we considered the problem of the MSNs deployment. Now, we optimize the MSNs' trajectories (i.e., MSNs speeds and their path lengths and locations) in detail. To do this, we first need an expression for the global probability of avoidance P_{GPA} (which is the complement of (13)). So, given a goal point $\mathbf{p}_g$ and a configuration of the MSNs, let us define the events: $\mathcal{I}(\mathbf{p}_g)$ and $\mathcal{E}(\mathbf{p}_g)$ respectively as the intruder completing its invasion and escaping phases without being intersected by any MSN. We have that:

$$\mathrm{P}_{GPA} = \mathbb{E}\left[\Pr(\mathcal{I}(\mathbf{p}_g) \cap \mathcal{E}(\mathbf{p}_g))\right] \tag{14}$$

where $\Pr(\mathcal{I}(\mathbf{p}_g))$ is the probability of occurrence of $\mathcal{I}(\mathbf{p}_g)$ and the expected value in (14) is taken with respect to $\mathbf{p}_g$ and the MSNs trajectories. Unfortunately (14) is not a suitable term to optimize because of its high computational complexity. So, we derive a more suitable and tractable approximation for (14) to be used in the WMSN optimization. From extensive simulations we observed that $\mathcal{I}(\mathbf{p}_g)$ and $\mathcal{E}(\mathbf{p}_g)$ are statistically dependent events. But, for tractability we approximate (14) by assuming $\mathcal{I}(\mathbf{p}_g)$ and $\mathcal{E}(\mathbf{p}_g)$ to be statistically independent:

$$\mathrm{P}_{GPA} \approx \mathbb{E}\left[\Pr(\mathcal{I}(\mathbf{p}_g))\right] \mathbb{E}\left[\Pr(\mathcal{E}(\mathbf{p}_g))\right] \triangleq \hat{\mathrm{P}}_{GPA} \tag{15}$$

Due to the symmetry of both intruder's phases we have that:

$$\hat{\mathrm{P}}_{GPA} = \mathrm{P}_{\mathcal{I}}^2 \tag{16}$$

$$\mathrm{P}_{\mathcal{I}} = \mathbb{E}\left[\Pr(\mathcal{I}(\mathbf{p}_g))\right] \tag{17}$$

where P_I in (17) is the probability that the intruder completes its invasion phase without being intersected by any MSN. We will refer to $\hat{\mathrm{P}}_{GPA}$ as a naive approximation for P_{GPA} because it is obtained by ignoring the statistical dependence between $\mathcal{I}(\mathbf{p}_g)$ and $\mathcal{E}(\mathbf{p}_g)$. But $\mathrm{P}_{\mathcal{I}}$ in (16) is still too complex for analytical or numerical calculation; so we continue our derivation for a suitable approximation of the global probability of avoidance.

[4] Many designs satisfy the proposed guidelines; simulation results show that these different designs did not lead to significant differences in the overall performance of the WMSN.

From (13) and (15) we approximate $\mathrm{P}_{\mathcal{I}}$ as follows[5]

$$\mathrm{P}_{\mathcal{I}} \approx \sum_{k=1}^{N_P} \bar{P}_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)\mathrm{P}_c(\mathcal{C}_k) \quad (18)$$

where $\mathcal{C}_k$ represents the event where the intruder crosses the convex hull of the sensing region associated with the k^{th} path; ℓ_k, $\mathbf{c}_k$ and ϕ_k represent respectively the length, center and orientation of the kth path; v_k represents the kth MSN speed; $\mathrm{P}_c(\mathcal{C}_k)$ is the probability that the intruder crosses the convex hull of the region sensed by the MSN(s) surveying the k^{th} path; $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ is the probability that at least one MSN intercepts the intruder when crossing the k^{th} path.

First of all, the event $\mathcal{C}_k$ is equivalent to the event in which the kth path is the closest path to the intruder's goal point $\mathbf{p}_g$. This comes from: the intruder's behaviour (see section II-A); the goal point's $\mathbf{p}_g$ uniform distribution within the ROI; and the MSN paths located close to the ROI perimeter. From those elements we can calculate $\mathrm{P}_c(\mathcal{C}_k)$ analytically using basic planar geometry (we omit these calculations because of lack of space and for the sake of the paper's clarity).

The probability $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ depends on the particular intruder's trajectory (which itself depends on $\mathbf{p}_g$) as well as on the position and orientation of the k^{th} path among other parameters. As opposed to $\mathrm{P}_c(\mathcal{C}_k)$, trying to calculate analytically $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ is extremely complicated and so numerical calculation is required. However, calculating $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ numerically for each path and for each iteration of the WMSN optimization process increases significantly the computational load making the optimization process computationally too demanding and even prohibitive in some cases.

To address this issue, we further simplify the problem by replacing $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ with another *naive approximation*. This approximation discards some of the dependencies of this probability on the intruder's trajectory and on the path location and orientation but keeps the dependency on the path length ℓ_k, the MSN(s) speed (v_k) and the number (M_k) of MSNs sharing the same path[6]. This is done to obtain an approximation which captures the behaviour of $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ but requires much less computation. We will refer to this new term as the naive local probability of intersection within the k^{th} path and write it as $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$. We formally define it as follows:

Definition. The local probability of intersection (P_{LPI}) for the k^{th} path of length ℓ_k when surveyed by M_k MSNs with speed v_k is defined as the probability (under constraints C1 and C2) that the intruder traverses the convex hull of the region sensed by the M_k MSNs assigned to the k^{th} path and comes within sensing range of at least one MSNs for at least one sampling instant.

(C1) the intruder's entry point follows a uniform distribution along one of the flat sides of the convex hull of the region sensed by the M_k MSNs associated to the k^{th} path (see the shape of the sensed region in Fig. 2).

(C2) the intruder moves on a straight line, orthogonal to the surveying path, from its entry point in one side of the convex hull to the other at constant speed v_I.□

The term $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$ is calculated numerically in two sets: one for $M_k = 1$ and another for $M_k = 2$. Each set is calculated for different values of v_k and ℓ_k with a fixed intruder's speed v_I and then stored in the form of lookup tables. This will significantly reduce the computational load in the optimization process.

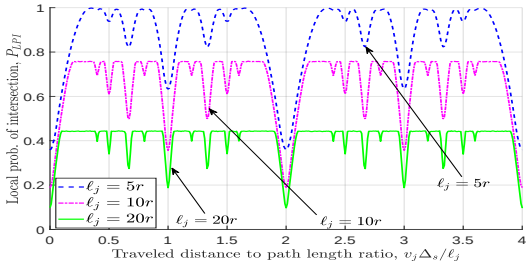

Fig. 5. Local probability of intersection (P_{LPI}) versus the ratio of the distance traveled by the MSN ($v_j\Delta_s$) over the j^{th} path length (ℓ_j) for one arbitrary MSN.

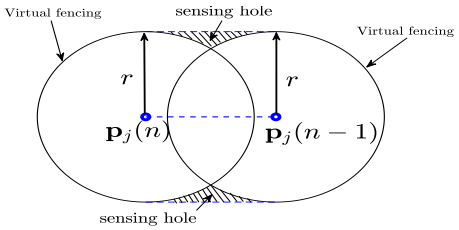

Fig. 6. Schematic illustration of the sensing hole phenomenon.

In Fig. 5 we observe $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$ for $M_k = 1$ and different values of v_j (normalized). The first thing we note is that P_{LPI} is a strictly increasing function of v_j only in an initial region. We also note that (P_{LPI}) is a periodic function of v_j with period of $\Delta_L = \frac{2\ell_j}{\Delta_s r_s}$. This periodicity implies the existence of a finite speed v_j that maximizes $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$ given that all the other parameters are fixed. This periodicity will also introduces multiple local maxima which might complicate the optimization process. To avoid this we constraint v_j as follows:

$$0 \leq v_j \leq V(\ell_k, M_k, v_I) \quad (19)$$

where $V(\ell_k, M_k, v_I)$ is the first value of v_j that produces a local maximum of $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$ given ℓ_k, M_k, v_I. Now, because the sensing is performed at discrete instants, *sensing holes* appear (see Fig. 6). Depending on the j^{th} MSNs speed (v_j), these sensing holes can vary in size. This is a reason for the periodicity observed in Fig. 5).

Now after deriving the approximation $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$ we continue to derive a tractable approximation for the global probability of avoidance P_{GPA}. To do this we replace, in the r.h.s. of (18), the term $P_I(\ell_k, \mathbf{c}_k, \phi_k, v_k, M_k|\mathcal{C}_k)$ with

[5]The approximation comes after neglecting the intersection between the sensing regions of adjacent paths. This approximation is reasonable if the average length of the paths is significantly longer than the sensing range r.

[6]These simplifications will significantly reduce the computational cost of the approximation for P_{GPA}

$\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$. Then, this approximation for $\mathrm{P}_{\mathcal{I}}$, which we denote $\tilde{\mathrm{P}}_{\mathcal{I}}$, is used in (16). We denote the resulting approximation as $\tilde{\mathrm{P}}_{GPA}$:

$$\tilde{\mathrm{P}}_{GPA} = \tilde{\mathrm{P}}_{\mathcal{I}}^2 \tag{20}$$

$$\tilde{\mathrm{P}}_{\mathcal{I}} \triangleq \sum_{k=1}^{N_P} \bar{\mathrm{P}}_{LPI}(\ell_k, v_k, M_k, v_I)\mathrm{P}_c(\mathcal{C}_k) \tag{21}$$

Using the approximation (20) will yield $sub-optimum$ solutions for the optimization of the WMSN, but will require much less computational resources than calculating numerically (14). As it will be shown in the simulations section $\tilde{\mathrm{P}}_{\mathcal{I}}$ in (20) constitutes a good approximation for $\mathrm{P}_{\mathcal{I}}$. However the approximation (20) presents a certain degree of error because we assumed in (15) that $\mathcal{I}(\mathbf{p}_g)$ and $\mathcal{E}(\mathbf{p}_g)$ are statistically independent (while they are not). Nevertheless, the approximation (20) is highly correlated to P_{GPA} making this naive approximation suitable to optimize the WMSN.

We next address the issue of designing the paths lengths and the MSNs' speeds. Towards this, we propose two methods that use (20) as a metric for the intruder's global probability of avoidance.

1) METHOD A: The WSN should be able to detect the intruder with high probability while efficiently using the MSN mechanical energy. To achieve this, in our first optimization method we minimize a convex combination of the naive approximation for the probability of avoidance (20) and the average motion power (3) spent by the MSN. The first term determines the network performance in detecting the intruder while the second term determines the lifetime of the network. So, the optimization problem can be stated as follows:

$$\begin{array}{l} \underset{\{v_k,\ell_k\}_{k=1}^{N_P}}{\text{minimize}} \quad \theta\tilde{\mathrm{P}}_{GPA} + \dfrac{(1-\theta)}{N}\displaystyle\sum_{k=1}^{N_P}\left\{M_k\left(\frac{v_k\Delta_s}{L_x}\right)^2\right\} \\ 0 \le v_k \le V(\ell_k, M_k, v_I) \end{array} \tag{22}$$

where Δ_s/L_x is a normalization constant[7]; $\theta \in [0,1]$ is a design parameter that determines the importance between minimizing the intruder's probability of avoidance (represented by its approximation $\tilde{\mathrm{P}}_{GPA}$) and minimizing the average power consumed by the MSNs. When $\theta = 0$, the optimization problem considers only minimizing the MSN's maximum consumed power, resulting in the MSNs being still; when $\theta = 1$, the optimization problem considers only the minimization of the intruder's probability of avoidance regardless of the energy consumed by the MSNs, resulting in a short-life time for the MSN.

If the probability of avoidance is high, the intruder will often invade the ROI undetected; the ROI will be unsafe. If the WMSN life-time is short the network will cease operation before the invasion of the intruder; the ROI will again be unsafe. So, in practice it is important to consider both the intruder's probability of avoidance and the energy consumed by the MSNs. This will improve the detection performance and prolong the WMSN's operational lifetime, thus significantly reducing the probability that an intruder invades the ROI. This trade-off is very interesting but out of the scope of this paper and will be investigated in future work.

The constraint on v_k is used to eliminate local optima and ease the optimization. The term $V(\ell_k, M_k, v_I)$ is calculated numerically from $\mathrm{P}_{LPI}(\ell_k, v_k, M_k, v_I)$ which, as mentioned previously, is stored as a lookup table prior to the optimization.

We remind the reader that the optimization problem above is solved by considering the path configuration discussed in section V-A (which also fixes $\{M_k\}_{k=1}^{N_P}$) and using the simulated annealing algorithm [29].

2) METHOD B: In our second method, we take a different approach. Our aim is to optimize the configuration of the WMSN to maximize the $network\ efficiency$. We define the $network\ efficiency$ as the ratio of the complement of $\tilde{\mathrm{P}}_{GPA}$ over the average MSNs' power spent. The $network\ efficiency$ is maximum when all the MSNs stay still (i.e., when $v_k = 0\ \forall k$). To avoid this, we introduce a penalization term to ensure that $\tilde{\mathrm{P}}_{GPA}$ approaches a certain value (a design parameter to be defined after (23)) as close as possible. So, the objective function to be optimized is:

$$F(g, P_{ref}) \triangleq \frac{1-\tilde{\mathrm{P}}_{GPA}}{\dfrac{1}{N}\displaystyle\sum_{k=1}^{N_P}\left\{M_k\left(\frac{v_k\Delta_s}{L_x}\right)^2\right\}} - \exp\left(\frac{g\left(\tilde{\mathrm{P}}_{GPA} - P_{ref}\right)}{\tilde{\mathrm{P}}_{GPA}}\right) \tag{23}$$

where both $g > 0$ and P_{ref} are the design parameters. The first term in (23) is the $network\ efficiency$ while the second term is the penalization term. Regarding the penalization term note that: when $g \to +\infty$, the penalization term subtracts infinity to the optimization target if $\tilde{\mathrm{P}}_{GPA} > P_{ref}$ but has negligible effect if $\tilde{\mathrm{P}}_{GPA} < P_{ref}$; when $v_k \to 0$ the network efficiency tends to $+\infty$ at the following rate $1/v_k^2$ but the penalization term tends to $-\infty$ at an exponential rate (see (20), (21) and Fig. 5) and so $F(g, P_{ref}) \to -\infty$ when $v_k = 0$ $\forall k$. Therefore, the penalization term acts as a $soft\ constraint$ on $\tilde{\mathrm{P}}_{GPA}$ and prevents the MSNs from remaining still. Finally, the optimization problem can be stated as follows:

$$\begin{array}{l} \underset{\{\ell_k,v_k\}_{k=1}^{N_P}}{\text{maximize}} \quad F(g, P_{ref}) \\ 0 \le v_k \le V(\ell_k, M_k, v_I) \end{array} \tag{24}$$

where g is a design parameter whose value must be sufficiently large. As before, this optimization problem can be also solved using the simulated annealing algorithm [29].

We have presented two alternative methods (namely METHOD A and METHOD B) for the optimization of the WMSN configuration. In the next section, we present the fusion rule for the FC.

VI. Simplified Fusion Rule-The Linear Approach

To reduce the communications burden the MSNs will report to the FC, at the end of their confirmation mode, only their positive local test statistic, see appendix B. For simplicity, we

[7]This normalization is for numerical convenience because $\tilde{\mathrm{P}}_{GPA}$ depends on $\{\frac{v_k\Delta_s}{\ell_k}\}_k$ rather than on $\{v_k\}_k$ alone, see (20), (21) and Fig. 5.

assume the error-free MSN-FC communications. The optimum fusion rule [5], [7] requires knowledge of intruder's parameters, which are unavailable to the WMSN, and also the MSNs exact locations[8] [27]. Hence, we develop a sub-optimum but simple fusion rule.

The global test statistic at the FC is taken to be the linear combination of all local positive test statistics received using a sliding window approach:

$$T_f(n;C_f) = \sum_{j=1}^{N} \sum_{k=n-C_f}^{n} T_j[k] \tag{25}$$

where C_f is the sliding window size (a design parameter). The FC assumes all non-received test statistics to be zero. Then, the FC makes a final decision by thresholding the global test statistic $T_f(n;C_f)$:

$$\left.\begin{array}{l} \text{if } T_f(n;C_f) < K, \text{decide } \mathcal{H}_0''[n] \\ \text{if } T_f(n;C_f) \geq K, \text{decide } \mathcal{H}_1''[n] \end{array}\right\} \tag{26}$$

where

$$\begin{aligned} \mathcal{H}_0''[n] : s_j[k] &= w_j[k] \qquad (27)\\ &\quad \forall\ k \in [n-C_f-C, \cdots, n-C] \\ &\quad \forall\ j \in \{1, \cdots, N\}, \\ \mathcal{H}_1''[n] : s_j[k] &= \tilde{a}\left(\mathbf{p}_j[k],\ \mathbf{p}_I[k]\right) + w_j[k] \qquad (28)\\ &\quad \text{for some } k \in [n-C_f-C, \cdots, n-C] \\ &\quad \text{for some } j \in \{1, \cdots, N\}. \end{aligned}$$

The hypothesis $\mathcal{H}_1''[n]$ implies the intruder's presence during the time interval $[(n-C_f-C)\Delta_s, \cdots, (n-C)\Delta_s]$. Information about the *intruder* or about the MSNs locations are unneeded. This simplifies the deployment of our proposed system.

The global probability of false alarm (P_{fa}^g) and the global probability of detection (P_d^g) are:

$$\begin{aligned} P_{fa}^g &= \Pr\left(T_f(n;C_f) \geq K | \mathcal{H}_0''[n]\right) \\ P_d^g &= \Pr\left(T_f(n;C_f) \geq K | \mathcal{H}_1''[n]\right). \qquad (29) \end{aligned}$$

where K is the threshold used by the FC. Clearly, (29) lacks a closed form solution and so we evaluate it numerically in the simulations section (see Section VII).

VII. Simulations Results

As mentioned before, one of the important properties of our optimization method is that we have decoupled, by introducing the probability of intersection, the optimization of the MSNs trajectories from the detection-related parameters. So, in the first part of this section, we present the performance of the optimized WMSN from the perspective of the global probability of intersection with the methods presented in section V. Then, in the second part we evaluate its detection performance.

For all the experiments of this section we consider a rectangular ROI of size $78r \times 40r$; on single intruder with speed $v_I = 0.3r/\Delta_s$ and sampling period $\Delta_s = 1$s.

[8]This needs the FC to continuously receive the MSNs' locations; having a high cost due to the transmission energy and thus making it impractical.

A. Impact of Approximations used in the Optimisation Procedures on the System Performance

Here, we constraint the MSNs to operate only on their surveying mode.

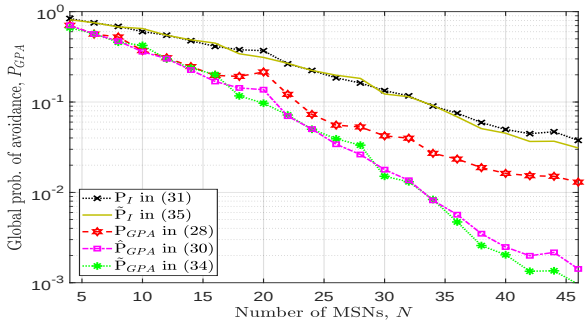

Fig. 7. Global probability of avoidance against the number of MSNs (N) after optimizing the WMSN according to (22) with $\theta = 1$ and MSNs synchronized.

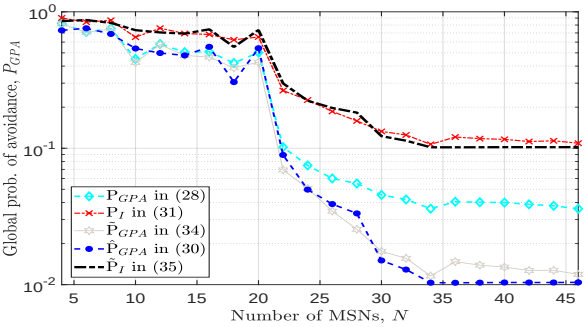

Fig. 8. Global probability of avoidance versus the number of MSNs (N) after optimizing the WMSN according to (24) with $P_{ref} = 0.01$ and MSNs synchronized.

In Fig. 7 and Fig. 8, we show the performance of the system optimized according to METHOD A with $\theta = 1$ and METHOD B with $P_{ref} = 0.01$ respectively. To get an insight into the impact of the approximations related to the global probability of avoidance imposed during the optimisation phase (see section V-B), in both figures, we plot P_{GPA} in (14) (measured by simulations), $\hat{\mathrm{P}}_{GPA}$ in (16), $\mathrm{P}_{\mathcal{I}}$ in (17) (measured by simulations), $\tilde{P}_{GPA}$ in (20) and $\tilde{\mathrm{P}}_{\mathcal{I}}$ in (21). It is clear that for both METHOD A and METHOD B, our proposed approximation $\tilde{\mathrm{P}}_{\mathcal{I}}$ follows closely $\mathrm{P}_{\mathcal{I}}$ which validates this approximation. However, the approximation $\tilde{P}_{GPA}$ of P_{GPA} aligns well only when the number of MSNs (N) is small (and so the path length of the MSNs is large). When N increases (and so the MSNs surveying path shortens), the approximation error increases. The non-alignment between $\tilde{P}_{GPA}$ and P_{GPA} is due to the fact that $P_{GPA} \neq \mathrm{P}_{\mathcal{I}}^2$ while $\tilde{P}_{GPA} = \tilde{\mathrm{P}}_{\mathcal{I}}^2$ (this is supported by the fact that $\tilde{P}_{GPA}$ follows $\hat{P}_{GPA} = \mathrm{P}_{\mathcal{I}}^2$ very closely). This shows that the events (described in section V-B) $\mathcal{I}(\mathbf{p}_g)$ (the MSNs failing to intersect the intruder before completing its invasion phase) and $\mathcal{E}(\mathbf{p}_g)$ (the MSNs failing to intersect the intruder before completing its escaping phase) are not statistically independent.

However, as mentioned in section V-B, we constructed

the approximation $\tilde{P}_{GPA}$ (for mathematical simplicity and tractability) assuming those events to be statistically independent, even though we knew they were not —this is the reason why we refer to $\tilde{P}_{GPA}$ as a naive approximation. We would like to clarify that regardless of the disparity between $\tilde{P}_{GPA}$ and P_{GPA}, the proposed approximation ($\tilde{P}_{GPA}$) remains always correlated to P_{GPA} and hence its utilization to represent the behavior of P_{GPA} in the optimization problems is adequate.

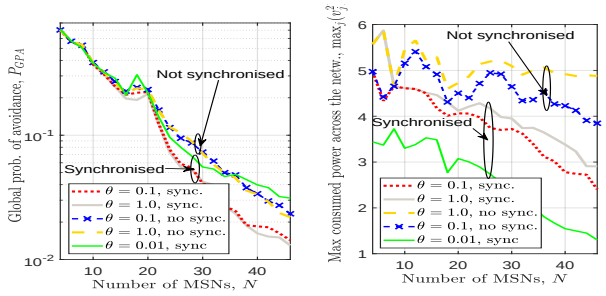

Fig. 9. a) Global probability of avoidance against the MSNs number (N) and b) Maximum consumed power across the network ($\max_j(v_j^2)$) against N for a network optimized according to (22) and MSNs synchronized with the method of subsection V-A.

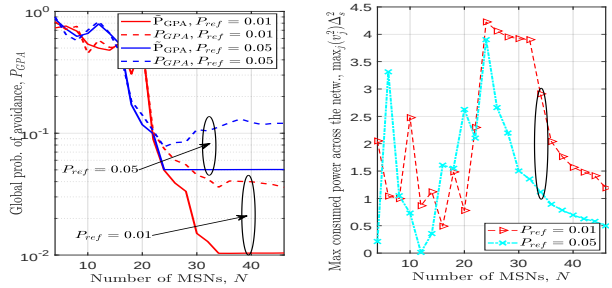

Fig. 10. a) Global probability of avoidance against the MSNs number (N) and b) Maximum consumed power across the network ($\max_j(v_j^2)$) against N for a network optimized according to (24) and MSNs synchronized with the method of subsection V-A.

We now evaluate the WMSN after deploying the MSNs using rules presented in section V-A and with the MSNs' speeds and path lengths optimized according to methods A and B presented in section V-B. In Fig. 9 and Fig. 10, we observe the measured global probability of avoidance (P_{GPA}) and the average MSNs power consumption against N.

In Fig. 9 we observe five scenarios: i) MSNs optimized according to method A with $\theta = 1$ and the trajectories of MSNs sharing the same path are synchronized according to the method described at the end of section V-A; ii) Similar to i) but with the MSNs sharing the same path having independent trajectories; iii) Similar to i) but with $\theta = 0.1$; iv) Similar to ii) but with $\theta = 0.1$; v) Similar to i) but with $\theta = 0.01$. When we compare i) with ii) and iii) with iv) we observe the benefit of synchronizing the MSNs: when the MSNs sharing the same path synchronize their trajectories the WMSN improves its performance both in terms of probability of avoidance and power consumption. This suggests the existence of other synchronization strategies (at larger scales) for MSNs having different surveying paths that could further improve the WMSN performance. The search for such synchronization strategies will be the subject of future research.

When comparing i), iii) and v), we observe that as θ increases, the probability of avoidance decreases and the average MSN power consumption also increases. In practice, θ values close to 1 would significantly reduce the probability of avoidance but also consume more energy and therefore reduce the WMSN operational time; reducing the probability that the WMSN would be fully operational when the intruder tries to invade the ROI. Low θ values would reduce the energy consumption significantly and increase the probability that the WMSN would remain operational once the intruder invades the ROI but the avoidance probability would be high. This is a complex tradeoff that should be investigated in more detail in future research by taking into account also the energy levels of the MSNs' batteries.

In Fig. 10 we observe two scenarios: i) WMSN optimized according to method B with $P_{ref} = 0.01$ and ii) Similar to i) but with $P_{ref} = 0.05$. In both scenarios the trajectories of MSNs sharing the same path are synchronized and we set $g = 8000$, see (23).

When N is small and $\tilde{P}_{GPA}$ cannot reach P_{ref} the performance of the WMSN is poor. This is due to the fact that in practice when $\tilde{P}_{GPA} \gg P_{ref}$ the penalization term in (23), used in the optimization process, takes extremely large values which saturate the variables which store the optimization target value within the computer. As a consequence when we use METHOD B and $\tilde{P}_{GPA} \gg P_{ref}$, the WMSN is not really being optimized. But, when $\tilde{P}_{GPA}$ can reach P_{ref} or stay close then we observe a more reasonable behavior, see $N \geq 24$ for $P_{ref} = 0.05$ and $N \geq 32$ for $P_{ref} = 0.01$ in Fig. 10. Once $\tilde{P}_{GPA}$ reaches P_{ref} it stays there while the average power consumption continues to decrease as the number of MSNs N increases. This maximizes the efficiency of the WMSN while satisfying the intended value for $\tilde{P}_{GPA}$. Due to the disparity between $\tilde{P}_{GPA}$ and P_{GPA} mentioned earlier, we observe that P_{GPA} also seems to converge but to a different (higher) value.

Now that we have evaluated the WMSN from the probability of avoidance perspective, we next evaluate its detection probability.

B. System Detection Performance

We consider $N = 24$ MSNs and for the sensor model we select: $P_I = 1$, $\sigma^2 = 0.2$ and $d = 0.1r$.

As previously mentioned, the *detection mode* duration (i.e., C) in (33) is an important design parameter that significantly affects the system detection performance.

In Fig. 11, we plot the ROC performance for various *detection mode* durations (C) and for a fixed detection threshold (K) in (26). Obviously, there is an optimum value of C such that P_d^g is maximized (for all the P_{fa}^g values). The detection performance for $C = 1$ in (33) (i.e., using the 1-sample local test statistic) is also plotted. This corresponds to the case where the MSN continuously surveys and performs the local detection $on - fly$ (i.e., no detection delay is introduced in (34)). Clearly, by appropriately choosing the

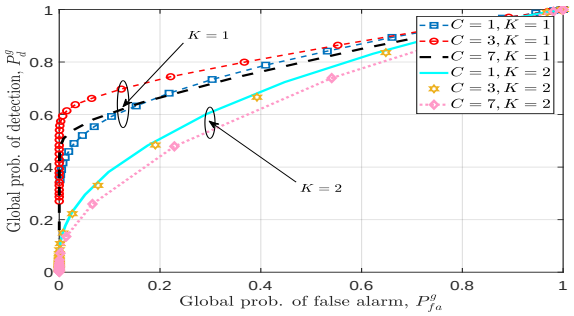

Fig. 11. Receiver Operating Characteristic against the $detection - mode$ duration C in (33), the MSNs optimized according (22) with $\theta = 0.9$, FC detection threshold ($K = 1$), sliding window size ($C_f = 22$) and $surveying - mode$ threshold ($\tilde{\Lambda}_j = 0.5, \forall j$).

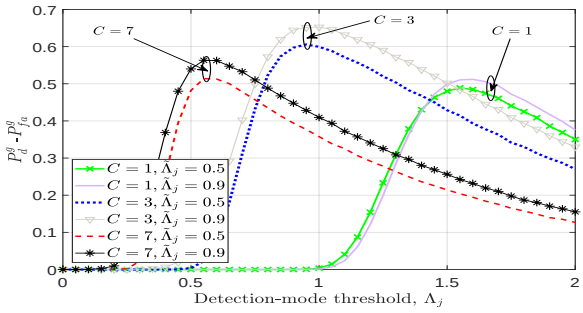

Fig. 14. The $P_d^g - P_{fa}^g$ metric versus the $detection - mode$ threshold (Λ_j) parametrized on the $detection - mode$ duration (C) in (33), with sliding window size ($C_f = 22$), detection threshold ($K = 1$), MSNs optimized according to (22) with $\theta = 0.9$.

$detection\ mode$ duration (C) (i.e., the MSN's stopping time $C\Delta_s$), the performance gain of the proposed detection scheme is significant compared to the scheme when MSN does not stop at all.

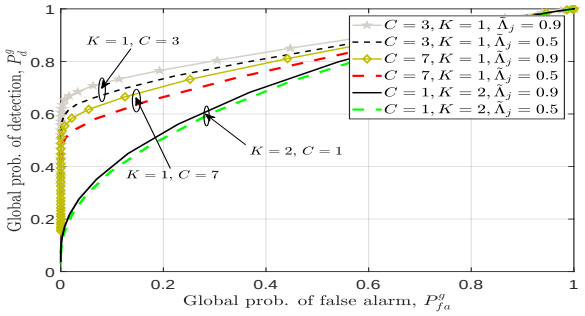

Fig. 12. Receiver Operating Characteristic against the detection threshold (K) and $surveying - mode$ threshold ($\tilde{\Lambda}_j$) in (32), the MSNs optimized according (22) with $\theta = 0.9$ and sliding window size ($C_f = 22$).

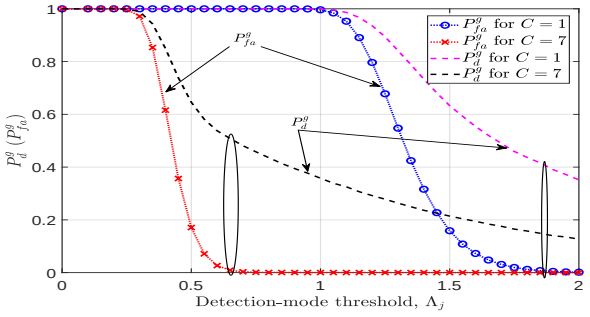

Fig. 13. Probability of detection (false alarm) P_d^g (P_{fa}^g) versus the $detection - mode$ threshold (Λ_j) in (34) parametrized on the $detection - mode$ duration (C), with sliding window size ($C_f = 22$), detection threshold ($K = 1$), $surveying - mode$ threshold ($\tilde{\Lambda}_j = 0.5$) in (32), MSNs optimized according to (22) with $\theta = 0.9$.

We now investigate the impact of the thresholding operation on the detection performance. In Fig. 12, we plot the Receiver Operating Characteristics for the proposed algorithm with decision fusion in (26) against the detection threshold (K) and $surveying - mode$ threshold ($\tilde{\Lambda}_j$) in (32). Obviously, for a pair of K and C, there is an optimum $surveying - mode$ threshold ($\tilde{\Lambda}_j$) in (32). For example, when $K = 1$ and $C = 3$, the optimum global probability of detection P_d^g is achieved for ($\tilde{\Lambda}_j = 0.9$).

In Figures 13 and 14 we plot the ($P_d^g - P_{fa}^g$) and the P_d^g/P_{fa}^g metrics, respectively, versus the $detection - mode$ threshold (Λ_j) parametrized on the $detection - mode$ duration (C). In Fig.13, we observe that for $P_{fa}^g = 0$, there is an optimum $detection - mode$ threshold (Λ_j) for which the detection probability is maximized. However, trying to further improve the detection performance would also increase the probability of false alarm. In general, different applications require different $acceptable\ P_{fa}^g$ rates. This determines the upper bound limit on the detection performance (e.g., for $C = 7$ and $P_{fa}^g < 0.2$, a maximum achievable detection rate of 0.65 only is possible).

Fig.14 shows the ($P_d^g - P_{fa}^g$) distance metric against the $detection - mode$ threshold (Λ_j). Note that ($P_d^g - P_{fa}^g$) is convex with respect to Λ_j. Clearly, there is a unique $detection - mode$ threshold (Λ_j) such that the ($P_d^g - P_{fa}^g$) distance is maximized for all C and $\tilde{\Lambda}_j$ values.

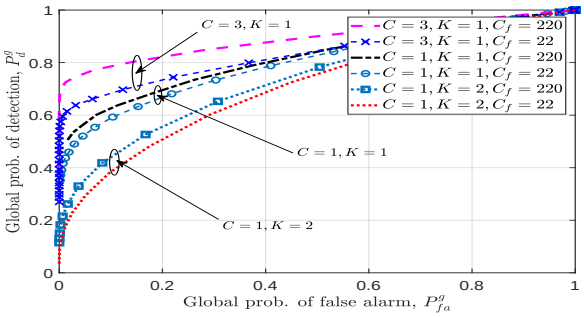

Fig. 15. Receiver Operating Characteristic against the sliding window size C_f in (25) parametrized on the $detection - mode$ duration C in (33) for the proposed algorithm with decision fusion in (22), FC detection threshold ($K = 1$), $surveying - mode$ threshold ($\tilde{\Lambda}_j = 0.5, \forall j$) in (32), MSNs optimized according to (22) with $\theta = 0.9$..

Now, we investigate the Receiver Operating Characteristic against the sliding window size C_f in (25). From Fig. 15 we note that the sliding window size plays an important role in the detection. For e.g., selecting $C = 3$, $K = 1$, and for an acceptable probability of false alarm of $P_{fa}^g < 0.2$,

a maximum detection rate of 0.75 and 0.82 for $C_f = 22$ and $C_f = 220$ respectively is achievable.

VIII. Conclusions

In this paper, we considered key issues related to intrusion detection in WMSN. We proposed a new $two{-}mode$ operation algorithm for the MSNs, and have shown that by optimizing the MSNs behaviour we can achieve higher intrusion detection and lower mechanical energy consumption, thus improving the network operational lifetime and performance. To make the optimization problems tractable, we made a number of approximations and evaluated their impact and their validity via simulations.

Future work will consider the case of a fully distributed WMSN, where the MSN collaborate among themselves to make a global decision without any fusion center.

Appendix A
Sensing for Surveying mode

Each MSN continuously senses its environment and performs local detection thresholding on its instantaneous samples. If the test performed by the MSN suggests the presence of the intruder then it switches to its $confirmation - mode$. From (5), the measured signal at MSN j is:

$$\begin{aligned} \mathcal{H}_0[n] : s_j[n] &= w_j[n], \quad (30) \\ \mathcal{H}_1[n] : s_j[n] &= \tilde{a}\left(\mathbf{p}_j[n],\ \mathbf{p}_I[n]\right) + w_j[n] \quad (31) \end{aligned}$$

with: $\mathbb{E}\left\{s_j[n]|\mathcal{H}_0[n]\right\}=0$; $\mathbb{E}\left\{s_j[n]|\mathcal{H}_1[n]\right\}=\tilde{a}\left(\mathbf{p}_j[n],\ \mathbf{p}_I[n]\right)$; and $\mathrm{Var}\left\{s_j[n]|\mathcal{H}_0[n]\right\} = \mathrm{Var}\left\{s_j[n]|\mathcal{H}_1[n]\right\} = \sigma^2$. Based on its j^{th} signal sample $s_j[n]$, the j^{th} MSN generates a binary test statistic $\tilde{T}_j[n]$ as follows:

$$\left.\begin{array}{l} \text{if } s_j[n] < \tilde{\Lambda}_j, \tilde{T}_j[n] = 0 \implies \text{decide } \mathcal{H}_0[n] \\ \text{if } s_j[n] \geq \tilde{\Lambda}_j, \tilde{T}_j[n] = 1 \implies \text{decide } \mathcal{H}_1[n] \end{array}\right\} \quad (32)$$

where $\tilde{\Lambda}_j$ is the local detection threshold during the $surveying\ mode$ for the j^{th} MSN.

When the j^{th} MSN suspects that the intruder might be present (i.e., $\tilde{T}_j[n] = 1$ in (32)), it switches to its $confirmation - mode$ so that a final local decision is taken.

Appendix B
Sensing for Confirmation mode

During the $confirmation\ mode$, the j^{th} MSN stops for a time $C\Delta_s$ to maximize its sensor output SNR (5) and reduce the uncertainty about the intruder's status. Then, the j^{th} MSN takes a local decision on the following local test statistic:

$$y_j(n_d^j; C) = \frac{1}{C+1} \sum_{n=n_d^j}^{n_d^j+C} s_j[n] \quad (33)$$

Then, the j^{th} MSN estimates the binary indicator variable at time instant $(n_d^j + C)\Delta_s$:

$$\left.\begin{array}{l} \text{if } y_j(n_d^j; C) < \Lambda_j, T_j[n_d^j + C] = 0 \implies \text{decide } \mathcal{H}_0'[n_d^j] \\ \text{if } y_j(n_d^j; C) \geq \Lambda_j, T_j[n_d^j + C] = 1 \implies \text{decide } \mathcal{H}_1'[n_d^j] \end{array}\right\} \quad (34)$$

where (for mathematical convenience) $T_j[n] = 0$ for $n \in \{n_d^j, \cdots, n_d^j + C - 1\}$ and Λ_j is the $confirmation - mode$ threshold for the j^{th} MSN. The thresholds used during the $surveying - mode$ ($\tilde{\Lambda}_j$) and $confirmation - mode$ Λ_j are in general different. For $n \in [n_d^j, \cdots, n_d^j + C]$ we have:

$$\begin{aligned} \mathcal{H}_0'[n_d^j] : s_j[n] &= w_j[n],\ \forall\ n \in [n_d^j, \cdots, n_d^j + C] \quad (35) \\ \mathcal{H}_1'[n_d^j] : s_j[n] &= \tilde{a}\left(\mathbf{p}_j(n),\ \mathbf{p}_I(n)\right) + w_j(n) \end{aligned}$$

The statistical moments of y_j are: $\mathbb{E}\left\{y_j|\mathcal{H}_0'[n_d^j]\right\}=0$; $\mathbb{E}\left\{y_j|\mathcal{H}_1'[n_d^j]\right\}=\sum_{n=n_d^j}^{n_d^j+C} \frac{\tilde{a}(\mathbf{p}_j[n],\ \mathbf{p}_I[n])}{C+1} \geq 0$; $\mathrm{Var}\left\{y_j|\mathcal{H}_0'[n_d^j]\right\} = \mathrm{Var}\left\{y_j|\mathcal{H}_1'[n_d^j]\right\} = \sigma^2/(C+1)$.

Once the one bit test statistic $T_j[n_d^j + C]$ is estimated, the MSN transmits it to the FC only if it is positive—to reduce the communications burden and the network energy consumption—and switches back to its $surveying - mode$.

References

[1] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks", *in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Salt Lake City, UT, United States, 7-11 May 2001.

[2] O. Songhwai, C. Phoebus, M. Michael, M. Srivastava, and S. Shankar," Instrumenting Wireless Sensor Networks for Real-time Surveillanc'e", *in Proc. of the Int.l Conf. on Robotics and Automation (ICRA)*, May 2006.

[3] E. Nurellari, D. McLernon and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules Via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," *in IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 3, pp. 321-335, Sept. 2016.

[4] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342-1363, thirdquarter 2015.

[5] E. Nurellari, D. McLernon, and M. Ghogho, "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks,* vol. , no. , pp. , May 2017.

[6] B. Kailkhura, S. Brahma and P. K. Varshney, "Data Falsification Attacks on Consensus-Based Detection Systems," in *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 145-158, March 2017.

[7] E. Nurellari, D. McLernon, M. Ghogho, and S. Aldalahmeh, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation," *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.

[8] X. Li, R.Falcon, A. Nayak, and I. Stojmenovic, "Servicing Wireless Sensor Networks by Mobile Robots", IEEE Communications Magazine, Vol. 50, Iss. 7, July 2012.

[9] A. Wichmann, B. D,Okkalioglu and T. Korkmaz, "The integration of mobile (tele) robotics and wireless sensor networks: A survey", Comp. Comm. 51 (2014) pp. 21-35.

[10] M. Rajesh, A. George and T.S.B. Sudarshan,"Energy Efficient Deployment of Wireless Sensor Network By Multiple Mobile Robots", *Proc. of the 2015 Int. Conf. on Computing and Network Comm. (CoCoNet)*, Trivandrum, India.

[11] T. Wang, Z. Peng, J. Liang, S. Wen, M. Z. A. Bhuiyan, Y. Cai, and J. Cao, "Following targets for mobile tracking in wireless sensor networks", in *ACM Transactions on Sensor Networks*, vol. 12, no. 4, Sep. 2016.

[12] P. N. Pathirana, N. Bulusu, A. V. Savkin and S. Jha,"Node Localization Using Mobile Robots in Delay-Tolerant Sensor Networks", *IEEE Trans. on Mob. Computing*, Vol. 4, 2005.

[13] C.T. Chang, et al., "Data Collection for Robot Movement Mechanisms in Wireless Sensor and Robot Networks", *Proc. of the 2016 Int. Computer Symposium (ICS)*, Chiayi, Taiwan.

[14] U. Baroudi, “Robot-Assisted Maintenance of Wireless Sensor Networks Using Wireless Energy Transfer," in *IEEE Sensors Journal*, vol. 17, no. 14, pp. 4661-4671, 15 Jul., 2017.

[15] D. Bonilla Licea, D. McLernon, M. Ghogho, E. Nurellari, and S. A. R. Zaidi, “Robotic Mobility Diversity Algorithm with Continuous Search Space”, in *26th European Signal Processing Conference (EUSIPCO)*, Rome, 2018.

[16] D. Bonilla Licea; D. McLernon; M. Ghogho, “Optimal trajectory design for a DTOA based multi-robot angle of arrival estimation system for rescue operations”, Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6800 - 6804.

[17] D. Bonilla Licea, E. Nurellari, and M. Ghogho, “Energy balancing for robotic aided clustered wireless sensor networks using mobility diversity algorithms”, in *26th European Signal Processing Conference (EUSIPCO)*, Rome, 2018.

[18] B. Liu, O. Dousse, P. Nain, and D. Towsley,“Dynamic Coverage of Mobile Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 2, February 2013.

[19] Satoshi Hoshino ; Takahito Ishiwata, “Probabilistic Surveillance by Mobile Robot for Unknown Intruders”, 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)

[20] Xin Zhou ; Weiping Wang ; Tao Wang ; Yonglin Lei ; Fangcheng Zhong, “Bayesian Reinforcement Learning for Multi-Robot Decentralized Patrolling in Uncertain Environments”, IEEE Transactions on Vehicular Technology (Volume: 68 , Issue: 12 , Dec. 2019).

[21] David Saldaña ; Reza Javanmard Alitappeh ; Luciano C. A. Pimenta ; Renato Assunção ; Mario F. M. Campos, “Dynamic perimeter surveillance with a team of robots”, 2016 IEEE International Conference on Robotics and Automation (ICRA).

[22] Alexander Jahn ; Reza Javanmard Alitappeh ; David Saldaña ; Luciano C. A. Pimenta ; Andre G. Santos ; Mario F. M. Campos, “Distributed multi-robot coordination for dynamic perimeter surveillance in uncertain environments”, 2017 IEEE International Conference on Robotics and Automation (ICRA).

[23] Song Gao; Rui Song; Yibin Li, “Cooperative Control of Multiple Nonholonomic Robots for Escorting and Patrolling Mission Based on Vector Field”, IEEE Access (Volume: 6).

[24] S. Marano, V. Matta, and L. Tong, “Distributed detection in the presence of byzantine attacks," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16-29, Oct 2009.

[25] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, “Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774-786, Jan. 2011.

[26] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, “Detection, classification, and tracking of targets”, *IEEE Signal Processing Mag.,* vol. 19, no. 2, pp. 17-29, 2002.

[27] R. Niu, P.K. Varshney, “Distributed Detection and Fusion in a Large Wireless Sensor Network of Random Size”, in *EURASIP Journal on Wireless Communications and Networking*, vol. 2005(4), pp. 462-472, 8 Sep. 2005.

[28] S. Aldalahmeh, M. Ghogho, D. McLernon, and E. Nurellari, “Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, vol. 2016(5), pp. 1-12, Jan. 2016.

[29] S. Russell, P. Norving, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 2003.

[30] D. E. Kirk, *Optimal control theory: An introduction*. Dover Publications, Inc., 2004.

[31] S. H. Javadi, “Detection over sensor networks: a tutorial”, in *IEEE Aerospace and Electronic Systems Magazine*, vol. 31, no. 3, pp. 2-18, March 2016.

PLACE PHOTO HERE

Daniel Bonilla Licea received his M.Sc. degree in communications from the Centro de Investigación y Estudios Avanzados (CINVESTAV), Mexico City, in 2011. From May 2011 until June 2012, he did an internship in the signal processing team of Intel Labs in Guadalajara, Mexico. He received his PhD degree in 2016 from the University of Leeds, U.K..Then, in 2016 he also participated into a short research visit at the Centre de Recherche en Automatique de Nancy (CRAN) in Nancy (France). In 2017 he collaborated in a research project with the Centro de Investigacion en Computacion (CIC) in Mexico. Currently he holds a postdoctoral position at the International University of Rabat in Morocco.

PLACE PHOTO HERE

Edmond Nurellari was awarded the Carter Prize for the best Ph. D. thesis, titled "Distributed Detection and Estimation in Wireless Sensor Networks: Resource Allocations, Fusion Rules, and Network Security", in the School in the year 2017-18, University of Leeds, UK. Since April 2017, Dr. Nurellari has been a faculty member with the School of Engineering at the University of Lincoln, United Kingdom, where he is currently a Senior Lecturer/Programme Leader in Electrical Engineering/Robotics. His research interests includes distributed signal processing, signal processing on graphs, resource allocations and distributed decisions in WSNs. He has served as an Invited Reviewer for the IEEE Trans. on Signal and Info. Process. over Networks, IEEE Communication Letter, Springers Wireless Networks Journal, Springers Digital Signal Processing Journal and IEEE Flagship conferences. Over the past few years, Dr. Nurellari has served as a Guest Editor of Special Issue "Smart Agricultural Applications with Internet of Things" for Sensors Journal, TPC Member for IEEE iSES, and a Reviewer for several UKRI grants including EPSRC and Future Leaders Fellowship.

PLACE PHOTO HERE

Mounir Ghogho received his MSc degree in 1993 and PhD degree in 1997 from the National Polytechnic Institute of Toulouse, France. He was an EPSRC Research Fellow with the University of Strathclyde (Scotland), from Sept 1997 to Nov 2001. In December 2001, he joined the University of Leeds where he was promoted to full Professor in 2008. In 2010, while remaining affiliated with the University of Leeds, he joined the International University of Rabat in 2010, where he is currently Dean of Doctoral College and Director of IT Research Laboratory (TICLab). He served as Dean of UIR’s Faculty of computer science and logistics in 2013. He is also currently Director of CNRS-Associated International Lab (LIA) DATANET, in the field of Big Data. He was elevated to the grade of IEEE Fellow in 2018, a recipient of the 2013 IBM Faculty Award and a recipient of the 2000 UK Royal Academy of Engineering Research Fellowship. His research interests are in signal processing, machine learning, data science, and wireless communication. He is currently a member of the steering committee of the Transactions of Signal and Information Processing. In the past, he served as an Associate Editor of many journals including IEEE Signal Processing Magazine and IEEE Transactions on Signal Processing, and a member of IEEE Signal Processing Society SPCOM, SPTM and SAM Technical Committees.

Mario Eduardo Rivero-Angeles (S'00-M'04) was born in Mexico D.F., Mexico, in 1976. He received the BSc degree from Metropolitan Autonomous University (UAM), Mexico, in 1998, the M.Sc. and Ph.D. degrees form CINVESTAV-IPN in 2000 and 2006 respectively in Electrical Engineering. He is a professor at the National Polytechnic Institute, currently at the Center of Research in Computation (CIC-IPN), Mexico since 2002. He was a Postdoctoral Fellow at Dyonisos research project in INRIA (Institut National de Recherche en Informatique et en Automatique), Rennes, France from 2007 to 2010. His research interest includes random access protocols and data transmission in cellular networks, P2P networks, and wireless sensor networks